SYSTEM SEGMENTATION

A FUNDAMENTAL CONCEPT FOR INDUSTRIAL CYBERSECURITY

UNISYS | Securing Your Tomorrow™

A FUNDAMENTAL CONCEPT FOR INDUSTRIAL CYBERSECURITY

Preface

Things are changing rapidly for the Industrial Control System (ICS) world, whether the operators want it to or not. More ICS devices are being connected to the Internet, which reduces the cost of operations and downtime but increases risk from hackers. Often in times of change, standards provide guidance and assurance about the ability to benefit from our connected world while reducing the associated risks. Unisys commissioned this paper by Eric Cosman on the application of "Cryptographic Zoning" (aka "microsegmentation") and the ANSI/ISA-62443 and IEC 62443 standards to highlight the advantages they may bring to the transitioning industrial world, including cloud deployment. We hope you will find it educational and informative.

1. Executive Summary

Industrial process and manufacturing plants are constantly evolving to meet the demand for new and improved products, or to respond to changing regulatory or business conditions. Processes have become more complex, requiring more sophisticated automation methods and technology to ensure their safe and reliable operation. Availability and integrity of the system under control (SuC) have always been an imperative in the operation of industrial control systems, but in recent years, requirements such as increased connectivity to and dependence on external systems have emerged. At the same time, the risks have increased to include deliberate or inadvertent compromise as result of inadequate cybersecurity. This new area of risk has also involved a much broader range of stakeholders. Both the number and sophistication of cybersecurity-related incidents have increased. In response to these and other developments, industrial control systems have also evolved to incorporate new technology in areas ranging from controller design to networking.

It has become imperative to understand, address and reduce the cybersecurity risk to industrial systems. This requires a combination of skills from several disciplines, ranging from process and automation engineering to network design and information security. Industrial systems have several characteristics that set them apart from normal business information systems. They typically use a complex mix of technologies and life cycles, tightly integrated with physical systems. They also tend to operate within very tight specifications, and may be intolerant to even small disturbances. Specific security related characteristics include the inclusion of components that cannot be patched or secured by conventional means, to the use of obscure and inherently insecure protocols.

Several of the common practices and methods used in information security are applicable to industrial systems, but they must be complemented with practices more tailored to this environment. Standards development organizations (SDO's) such as the International Society of Automation (ISA) have developed formal standards and practices for industrial cybersecurity. These standards define several fundamental concepts that are necessary for an effective response. These concepts include system segmentation (i.e., zones and conduits) and the assignment of security levels. This paper describes one approach to applying these concepts to improve the security of an existing system, as well as potentially applicable technologies and areas for future improvement.

The primary intended audience for this information includes both asset owners (or end users) and system integrators.

2. The Evolution of Industrial Control

Industrial control systems have changed and evolved almost continuously since the adoption of electronic controls several decades ago. While some of the changes have been internally driven in response to changing needs and advancing capability, others have been imposed or influenced by external trends and developments.

Ensuring the availability and integrity of these systems and the confidentiality of the data that they contain has become a major imperative in recent years. While this has always been of prime importance within operations, there is now an increased level of awareness and scrutiny from a much wider range of stakeholders. To meet this challenge, it is essential to understand how industrial control systems have evolved.

2.1. From Simple to Complex Control

The applications for industrial control systems (ICS) have changed considerably over the past several decades. Individual electronic controllers were first connected to minicomputers for process monitoring and supervisory control. These custom-built configurations quickly gave way to distributed control systems (DCS), while still coexisting with programmable logic controllers (PLC's). As the technical capabilities of these systems increased, the control applications have become more sophisticated and complex.

2.2. Technology Changes

One of the most significant trends has been the replacement of custom or purpose-built systems and components with commercial-off-the-shelf (COTS) technology. The impact has been seen in hardware and software used at the system, component, network and device levels. Market pressures have forced suppliers to replace expensive and inflexible proprietary hardware and software with general purpose personal computers and COTS systems software (i.e., UNIX and Windows).

Coincident with these platform changes, changes have occurred in networking and communications as proprietary protocols were supplanted first by Ethernet as a physical transport, and finally by TCP/IP. Various types of gateways and similar devices are now available to connect these newer networks to legacy systems. The result of these changes is increased diversity and complexity of industrial networks. Such networks are often configured with functionality as the primary concern, with much less care given to their operation and management.

2.3. From Connectivity to Dependence

Advances in capability and function often come with an increase in the interconnection of components, and associated system complexity. The cumulative result of these changes is that current industrial control systems are a complex "system of systems," including both individual components and more complete solutions that are based on a variety of technologies, with a wide range of capabilities and associated vulnerabilities and limitations.

2.4. External Integration

Improvements to supply chain and related business processes have led to increased demand for the connection of industrial control systems to higher level information systems. While many control systems still do not include external connections, there are many drivers for increased external access to process data, including:

- Production optimization across multiple facilities
- Enabling just-in-time manufacture and delivery
- Remote monitoring of the control systems for support purposes
- Optimization of utility costs and usage
- Real-time reporting of production results
- Regulatory and environmental monitoring

2.5. Security Incidents

The combination of the above trends and developments, combined with a general increase in the number and sophistication of cybersecurity attacks, has led to an increase in the number of cybersecurity incidents affecting industrial systems. The Repository for Industrial Security Incidents (RISI[1]) is one database of reported security incidents in control and SCADA systems. An analysis of the data from 1982 to 2010 found that the type of incidents affecting control systems breaks down as follows:

- 50% of incidents were accidental
- 30% of incidents were malware-based
- 11% of incidents were external attackers
- 9% of incidents were internal attackers

[1] *http://www.risidata.com/*

3. The Industrial Cybersecurity Imperative

Ensuring the safe and reliable operation of industrial processes has long been a major focus of the automation profession. Dedicated safety systems are employed where warranted, and their design and operation is governed by requirements stated in international standards such as IEC 61508 and IEC 61511.

With increased connectivity and visibility comes additional challenges in ensuring safe and reliable operation in the face of potential cybersecurity threats. Specifically, there is an increased risk of compromise via some combination of deliberate attack using malicious software and collateral impact from non-targeted malware.

The imperative is to mitigate, if not prevent such attacks and any resulting negative consequences. Methods and tools used for general purpose IT security may be useful for this purpose, but in most cases, they must be employed with specialized expertise, and possibly with other tools developed for this environment.

3.1. Domain Characteristics

The industrial control systems domain has several characteristics that present specific challenges in addressing their security. While there are challenges in each of the areas of people, process and technology, the focus of this discussion is limited to technology.

Multiple Technologies – A typical industrial control system has been assembled and modified over an extended period, and includes a variety of products and technologies. These products may be from multiple suppliers, installed over a period of many years as part of regular expansions or improvements. Many of the older products and technologies (e.g., protocols) were originally developed with little or no thought given to security. Those security features and capabilities that do exist may not be compatible with other parts of the extended system or network. In many cases, they have been disabled or otherwise defeated.

The typical control system grows and evolves over time as new opportunities and applications are identified. Examples include the layering of multi-variable control and optimization on top of the basic control system, or the addition of various types of performance monitoring and improvement solutions.

Complex Life Cycles – Each of the major components of a typical control system have a separate life cycle, corresponding to when it was purchased and installed. Coordination of these life cycles and making the necessary decisions about acquisition, removal and replacement can be particularly difficult for the asset owner.

Complex Networks – Industrial control systems are often very complex, including equally complex networks. Operations and control engineers often focus on functionality, giving much less consideration to the underlying infrastructure. Many asset owners have extensive control systems that are inadequately documented and poorly understood. Many of the components of these systems simply cannot be secured using modern methods and tools, either because they are obsolete, or because their function would be compromised by the addition of these capabilities.

It is possible to improve the security of industrial systems by applying the right combination of common practices and domain-specific measures.

3.2. Configuration Challenges

Although the situation is far from hopeless, there are challenges associated with properly securing industrial systems. Some of these are direct consequences of the above technical characteristics, while others are related to how such systems have typically been configured, installed and operated.

Perhaps most problematic is the fact that many – if not most – of the existing systems are configured for availability and performance, with little or no regard to cybersecurity. This approach was common and even acceptable for older systems, where there was little or no connectivity to external networks and systems.

Business and operational needs such as supplier support, remote monitoring and the need to access process data have led to a proliferation of external connections, each of which presents a possible point of entry for potential attackers or malicious software. Subsequent connections and integration have quickly revealed many "soft" targets that are inherent to these systems. Once they are accessible via networks, they may have very little capability to reject improper connections and commands. Some devices may crash if they receive malformed network traffic or even high loads of correctly-formed data. An additional complication is that computers in these networks often run for months without security or antivirus updates, and are susceptible to outdated malware.

Legacy industrial control systems have typically grown and expanded over time, as new features and capabilities have been added, or as the scope of control has expanded. There is an implicit level of trust within such systems, and they are seldom segmented by function or risk (the exception being safety systems).

3.3. Security Challenges

Information security experts (internal or external) may suggest that the application of common preventative measures can easily improve the security posture for industrial systems. While there is some truth to this assertion, it is important to understand the specific challenges associated with this environment before making such changes. These include:

Patching – It is often difficult or even impossible to apply patches to industrial systems using normal methods. Any proposed patches must be thoroughly tested on laboratory or development systems before applying them to production systems, since the consequence of a malfunction can include failure of or damage to physical equipment.

Protocols – Industrial networks may use unique communication protocols not seen in the IT world and not addressed by IT security products.

Monitoring Disruption – The simple act of monitoring of system components can result in interruptions, particularly if it involves active polling of what are often very "brittle" components. It may not be practical to add any sort of agent to such components, because of memory or processing constraints.

Suitability for Use – Industrial systems are typically operated and maintained by production personnel (i.e., engineers, technicians and operators) who are not cybersecurity experts. In many cases they may see security as an impediment to performing their normal duties. For this reason, security tools and procedures must be tailored for the environment.

Safety Systems – Safety systems have much different requirements and constraints with respect to availability, performance, change control, and access.

Complex Methodology – The methodology and techniques used to design, configure and maintain control systems can be very complex, requiring very specialized expertise. Such expertise may not always be readily available, particularly in a traditional IT support organization.

Distributed Systems – Industrial control systems – particularly Supervisory Control and Data Acquisition (SCADA) systems – are deployed across a broad geographical area. The communications links used to connect the various elements may have a lower level of trust and availability, which would require the creation of different zones.

4. Industry Response

In response to the need to improve the security of industrial control systems and associated data, industry has developed a variety of resources that capture practices and standards. These include guidance and recommended practices from government and industry associations, case studies, both sector-specific and general standards, and certification specifications.

4.1. Common Practices

There are several common, well-established practices in information security that can also be applied to some degree to industrial systems. Examples include:

Role-based Access – Granting access based on well-defined roles (rather than individuals) is a well-established practice that transfers easily to the industrial environment. Industrial applications must allow for the fact that roles are commonly shared, and may not have well-defined boundaries.

Least Privilege – If clear role definitions exist, this practice applies well in the industrial environment.

Risk Assessment – This is an essential first step in any security program. It applies very well to the industrial systems environment, but emphasis must be given to the consequence element of risk, since possible consequences extend well beyond loss of information.

Defense in Depth – This practice is particularly relevant for industrial systems, since they are deeply embedded within a larger enterprise, and may not be generally accessible from external sources.

Tools exist or are being developed to facilitate these and related practices. Some of these can be adapted from other domains, while others must be tailored to the industrial environment.

4.2. Supplement for the Domain

These and other practices are suitable for application in the industrial environment, but there are characteristics and constraints that must be considered. These are defined in the form of established and developing practices, guidelines, and standards.

Practices - Typically, the first result of applying processes and technology to a new situation is the emergence of proven practices. Depending on the circumstances, they may be captured in the form of some combination of guidelines and procedures. If relevant standards already exist, practices may be used to interpret normative requirements and provide specific guidance and direction on how these requirements are best met. Practices may also be adapted from similar documents developed for other contexts or environments, retaining the essential content and restating or interpreting it in another context.

Frameworks – Frameworks describe a context or structure within which practices and standards may be consistently applied. They do not define normative requirements, but include references to proven sources of this information. In the area of cybersecurity, the NIST Cybersecurity Framework (CSF) has been widely promoted and accepted since its creation. Its use is effectively mandated for U.S. government systems, and many private sector companies have adopted it as the basis of their cybersecurity management systems. This framework addresses all types of information systems, and is not specific to industrial systems.

Training and Certificates – It is also essential to address the "people" element of the traditional People, Process and Technology triad. This is commonly accomplished through a combination of training and certificates or certification that provide an objective assessment of capability.

4.3. Standards

Standards are a critical element of the cybersecurity response. Typically, they define "what" must be done to meet a specific performance level, in the form of normative requirements, without being too prescriptive in defining "how" it is to be done. Unfortunately, the term standard is often applied rather loosely to a wide variety of guidance and directive sources. It is important to understand the "standards" come in several forms. Each has a specific purpose or intent, as well as associated limitations.

Sector-Specific Standards – It is common for standards to be developed and offered for applications within a specific industry sector. The most notable example of a cybersecurity standard of this type is the NERC CIP series of standards for the Energy sector. Because they are developed by and for a single sector, standards of this type may have limited application in other circumstances.

Regional or National Standards – Standards may also have an implicit or explicit geographical focus. The obvious example of standards of this type are national standards. These may be adapted from, or used as the basis for international standards.

Functional or Technology Standards – Standards also have a defined scope in terms of functionality or technology. Some cybersecurity standards have a scope that is limited to specific subsets of the full automation solution, while others are more comprehensive.

The focus and intent of each of these types of standards can be combined to create international standards that are applicable across a broad range of sectors and technology.

5. ISA99 and 62443

In 2002 the International Society for Automation (ISA) recognized the need to address cybersecurity in its portfolio of industry standards. The result was the formation of the ISA99 committee to develop one or more standards for industrial automation and control systems cybersecurity. Since its formation, the ISA99 committee has developed a detailed roadmap that includes thirteen standards and technical reports on the subject.

These standards have been built on a solid foundation that includes the following fundamental concepts:

- Security life cycles
- Zones and conduits
- Security levels
- Program maturity
- Security and safety

5.1. The Basis for System Segmentation

Two of these fundamental concepts are of particular importance to systems integrators and asset owners. Zones and Conduits, and Security Levels are essential components of a risk-based approach to securing industrial control systems. They are closely related, in that the definition of segments or zones must be based on a careful assessment of target security levels, based on the vulnerability and consequence elements of risk. Both the zones and conduits and security levels concepts are addressed in detail in the ANSI/ISA 62443 standards.

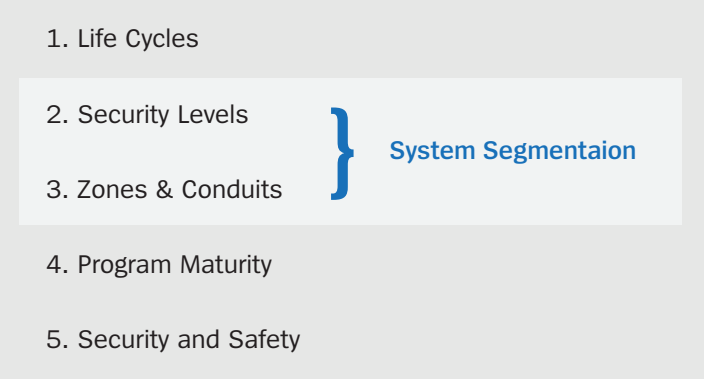

Figure 1 – Segmentation Concepts

5.2. Security Levels

Security-related features and countermeasures must be selected and implemented based on an assessment of perceived or expected risk. Since a range of responses are typically possible, there must be a method for determining the most appropriate response for a specific set of circumstances.

The security levels defined in the 62443 standards provide a qualitative approach to addressing security for a zone. As more data becomes available and the mathematical representations of risk, threats, and security incidents are developed, this concept will move to a quantitative approach for selection and verification of Security Levels (SL). It will be used to select IACS devices and countermeasures to be used within a zone and to identify and compare security of zones in different organizations across industry segments.

The standards describe security levels using a simple four-point scale, based on the nature of the risk, as shown in figure 2.

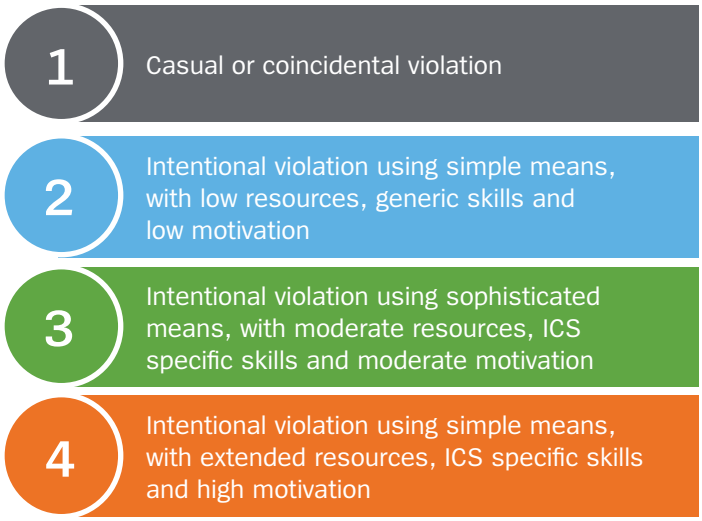

Figure 2 – ISA-62443 security levels

Using this scale, risk is described in terms of a combination of means, resources, skills and motivation. Other scales are also possible. For example, in some situations it may be preferable to define security levels in terms of the potential consequences.

5.3. Zones and Conduits

For all but the simplest of systems, it is not practical to assign a single security level to all components. Complex control systems may have many controllers and related components, applied to a variety of applications. Perhaps the most obvious example is the use of separate controllers for safety-critical applications. Different security levels may also be appropriate based on the nature of the process or the materials being processed.

Grouping system components into zones is used to identify those which share common security requirements and to permit the identification of common security measures required to mitigate risk. The assignment of components to zones and conduits may be adjusted based upon the results of the detailed risk assessment.

5.4. Normative Requirements

While valuable, the concepts described in the 62443 standards are not sufficient. They are complemented by a comprehensive set of normative requirements that define specific characteristics and actions that must be taken to secure the control system.

6. Applying the Segmentation Concept

In most – if not all – situations, there will be some need for communication between the industrial control system and external information systems or databases, which obviates the traditional "air gap" approach to protection. Even without such external connections, larger control systems – already complex at the time of installation and commissioning – will almost certainly evolve to meet changing requirements, involving the addition, modification or even the removal of components or subsystems. These changes will in turn require changes to the connectivity between components of the system. Some combination of internal and external connections will naturally lead to the need for segmentation.

Although each of the individual concepts described in the previous section is relatively straightforward, their combined application in a real situation can seem quite daunting. When considering such an application there are several key elements addressed in the 62443 standards.

Control system components are segmented into independent zones, composed of interconnected devices that work closely together to achieve a specific function. Communications within a zone are typically less restricted, but communication between zones must occur through a single point called a conduit, which is usually protected using devices such a secure router or firewall. Conduits must be configured to transmit only the data that is needed to coordinate the functions of the different zones. Any communications that are irrelevant to the function of a certain zone must be blocked.

While the exact process used for system segmentation will vary somewhat for each situation, there are several tasks or steps that are essential for obtaining the best results. One possible approach is shown in figure 3.

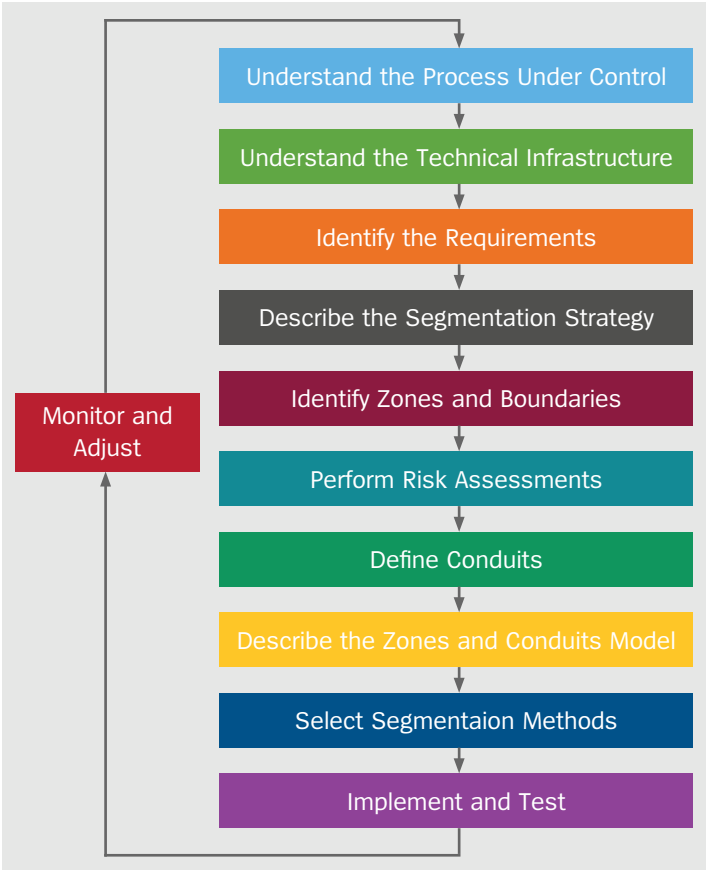

Figure 3 – Segmentation Approach

The tasks shown in this figure are described in more detail in the following paragraphs.

6.1. Understand the Process

The first step is the one most often overlooked by those who may not be familiar with industrial systems and networks. To fully understand and appreciate what is required to segment a control system and associated networks, it is first necessary to understand the physical process and system under control (SUC), as well as the logic that has been developed to automate it.

The process and equipment may be described in documents with names like “process description” or “process overview.” Although these may take the form of narrative descriptions, it is more common for them to some combination of diagrams and tables giving design conditions. The logic used to control the equipment may be available in a variety of forms, ranging from narrative documents to logic diagrams or even computer source code. Such documents may have names such as “control system design” or “automation strategy.” The information in these documents helps in the design of more resilient networks and segmentation of the controllers. It also defines what normal network traffic should look like.

Even with access to such documents it may not be possible to fully understand the physical process without assistance from a production or control engineer or operations staff responsible for its operation. It is quite common – especially with older facilities – for the above documents to be out of date, or simply not available.

Although gaining the necessary understanding of the production processes may take considerable time and effort, it is critical to have this information as the basis of any segmentation effort.

6.2. Understand the Technical Infrastructure

It is also essential to fully understand the information infrastructure; particularly the design and configuration of the network(s). The skills and experience required for completion of this task are typically more aligned with those of security experts. In some cases, the asset owner or support provider may have complete and accurate network diagrams and an associated database of information system components, such as routers, switches, servers, etc. Unfortunately, this is not a common situation, so some discovery and characterization may be required. This can be accomplished by usual manual methods, or by using scanning tools, if it is proven that their use will not disrupt normal operation. In general, such tools must operate in a totally passive mode.

6.3. Identify Requirements

At this point the current situation should be fully documented. It forms the starting point for additional segmentation. Before making recommendations or decisions it is essential to document the expectations and requirements. Some of these are apparent based on the nature of the functions performed (e.g., safety systems), while others may require more detailed investigation. It is particularly important to identify any data flows that are essential to proper operation. These will typically translate to conduits with one or more channels.

6.4. Describe the Segmentation Strategy

Even with an appreciation and detailed understanding of the current systems and requirements, effective segmentation consists of more than simply grouping components into zones. It is necessary to have a detailed segmentation strategy to ensure the success of the implementation. This strategy must clearly describe the intent behind the segmentation, based on the needs and constraints of the business processes and system under control.

For larger networks, most network architects or engineers will focus first on the larger network zones (e.g., DMZ, Core, Data Center, WAN, Campus, etc.). However, segmentation of industrial systems must consider operation and internal data flows between individual components.

The facility must first be divided into operational areas, such as materials storage, processing, finishing, etc. Operational areas can often be further divided into functional layers, such as manufacturing execution systems (MES), supervisory systems, and primary control systems (e.g., DCS. RTU, PLC). The general reference model in the 62443 standards is often used as a basis for this division. Vendor reference architectures can also be helpful.

The ISA-62443 and IEC 62443 standards describe how to develop a zone and conduit strategy based on the needs and constraints inherent in the industrial control system. Special attention should be given to the safety related systems including safety instrumented systems, wireless systems, systems directly connected to Internet endpoints, systems that interface to the IACS but are managed by other entities (including external systems) and mobile devices.

There are several other factors that may influence the segmentation strategy.

Network Performance – Devices used to connect zones must have the level of network performance needed to filter and deliver all data without impacting network availability.

Deep Packet Inspection – Devices at zone boundaries must be able to inspect the content of the packets of industrial protocols for abnormalities and security threats.

Deployment Complexity – The larger number of routers, firewalls or similar devices required to protect ICS networks translates to additional effort for their operation and support.

A well-crafted strategy must identify and define the following elements:

- Zones that account for all ICS assets
- Channels or means of data transfer including mobile transfers
- Conduits that include all discovered channels
- Controls for the flow of information between zones and within all conduits in the facility

6.5. Identify Zones and Boundaries

Zones and conduits are a means of restricting access to and information flow between systems, to improve the security and reliability of the overall system(s). If the logical perimeter doesn't adequately control access to the devices it contains, the system remains vulnerable.

Industry standards may not specify exactly how to define zones or conduits. Instead, they provide normative requirements that describe how to accomplish this based on an assessment of risk from cyber attack. Since risk is a function of the possibility of a cyber incident plus its consequences, the zones and protection needed will vary for each facility.

The ANSI/ISA-62443 standards define a zone as a "*collection of entities that represents partitioning of a System under Consideration on the basis their functional, logical and physical (including location) relationship.*" Each element of a zone has a security level capability. If the capability level is not equal to or higher than the requirement level, then extra security measures (e.g., implementing additional technology or policies) may be required.

The zone definition or description may be expressed either in terms of physical devices (i.e., physical zone), or in a logical manner (i.e., virtual zone). Virtual zones are defined by grouping assets, or parts of physical assets, into security zones based on functionality or other characteristics, rather than the actual location of the assets.

There can also be zones within zones, or subzones, that provide layered security. Such defense in depth can also be accomplished by assigning different properties to security zones. Zones may be viewed as trusted or untrusted.

6.5.1. Criteria

Zones must be defined using a variety of criteria, depending on the specific situation. Possible criteria include:

- Performance
- Data sensitivity
- Specific safety constraints
- Media used (e.g., wireless)
- Ability to patch or update

When defining a security zone, it is first necessary to assess the security requirements (security goals) as defined in the segmentation strategy. These are in turn used to determine whether a particular asset should be considered within the zone or outside the zone. The security requirements can be broken down into the following types:

Communications Access – For a group of assets within a security border to provide value, there must be links to assets outside the security zone. This access can be in many forms, including physical movement of assets (products) and people (employees and vendors) or electronic communication with entities outside the security zone. Remote communication is the transfer of information to and from entities that are not in proximity to each other. For purposes of this document, remote access is defined as communication with assets that are outside the perimeter of the security zone being addressed. Local access is usually considered communication between assets within a single security zone.

Physical Access and Proximity – Physical security zones are used to limit access to an area because all the systems in that area require the same level of trust of their human operators, maintainers, and developers. This does not preclude having a higher-level physical security zone embedded within a lower-level physical security zone or a higher-level communication access zone within a lower-level physical security zone. For physical zones, locks on doors or other physical means protect against unauthorized access. The boundary is the wall or cabinet that restricts access. Physical zones should have physical boundaries commensurate with the level of security desired, and aligned with other asset security plans.

Assets that are within the security border are those that must be protected to a given security level, or policy. All devices that are within the border must share the same minimum level of security requirements. In other terms, they must be protected to meet the same security policy. Protection mechanisms can differ depending on the asset being protected.

Assets that are outside the security zone are – by definition – at a lesser or different security level. They are not protected to the same security level, and cannot be trusted to the same security level or policy.

6.5.2. Attributes

Each zone is defined in terms of specific characteristics. These include ...

- zone description (name, definition, function),
- zone boundaries,
- typical assets and inventory,
- inheritance from other zones,
- zone risk assessment (e.g., security capabilities, threats, vulnerabilities, consequences, criticality),
- security objectives and strategy,
- acceptable use policy,
- inter-zone connections (i.e., access requirements), and
- the change management process.

6.6. Perform Risk Assessments

With all system assets assigned to zones, it is possible to conduct risk assessments for each of these zones. Risk must be considered in terms of each of its major components, as defined in figure 4.

$$\text{Risk} = f\,(\text{Threat, Vulnerability, Consequence})$$

Figure 4 – Risk Calculation

Every industrial control system presents a different risk to the organization depending upon the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system and the consequences if the system were to be compromised.

Information about potential threats and vulnerabilities is readily available from a variety of government or private sources, such as cyber event response teams (e.g., ICS-CERT), suppliers or cybersecurity researchers. For the most part, the threats and vulnerabilities associated with industrial control systems are the same as those for any electronic information systems.

It is the consequence element that differentiates the risk for industrial systems. Since these systems are typically attached to physical processes and equipment, the consequences often include malfunction, damage or loss of control of these processes, as well as possible damage to the surrounding environment.

The ISA-62443-3-2 standard[2] (Security Risk Assessment, System Partitioning and Security Levels) defines a set of engineering measures that guide an organization through the process of assessing the risk for each of the zones in a specific system and identifying and applying security countermeasures to reduce that risk to tolerable levels.

6.7. Define Conduits

Information must flow into, out of, and within a security zone. Even in a non-networked system, some communication exists (e.g., intermittent connection of programming devices to create and maintain the systems). To cover the security aspects of communication and to provide a construct to encompass the unique requirements of communications, the 62443 standards define a special type of security zone: a communications conduit.

A conduit is a type of security zone that groups communications that can be logically organized into a grouping of information flows within and external to a zone. It can be a single service (i.e., a single Ethernet network) or can be made up of multiple data carriers (multiple network cables and direct physical accesses). As with zones, it can be made of both physical and logical constructs. Conduits may connect entities within a zone or may connect different zones.

Any communications between zones must be via a defined conduit. Conduits control access to zones, resist denial of service attacks or the transfer of malware, shield other network systems and protect network traffic integrity and confidentiality. Typically, the controls on a conduit are intended to mitigate the difference between a zone's security level capability and its security requirements. Focusing on conduit mitigations is typically far more cost effective than having to upgrade every device or computer in a zone to meet a requirement.

Data flow diagrams are useful for summarizing the conduits and traffic flows they contain. Each zone can be represented by a node and each flow can be represented by a vector.

Traditional segmentation mechanisms that use virtual networks or routing could either limit the amount of zone separation (by using too few devices), or become unduly complex (requiring massive network redesign). Too simple, and the right security isn't implemented in the right places; too complex, and the risk of misconfiguration can result in less effective security and unintentional vulnerability. The complexity of highly sub-networked or virtual network-separated systems also requires administrative overhead to operations teams, who are already strapped for IT skills and resources. System suppliers may also dictate specific designs, making the implementation of new network segmentation contractually impossible.

Channels are the specific communication links established within a communication conduit. Channels inherit the security properties of the conduit used as the communication media (i.e., a channel within a secured conduit will maintain the security level of the secured conduit).

6.7.1. Attributes

As with zones, conduits may be either trusted or untrusted. Conduits that do not cross zone boundaries are typically trusted by the communicating processes within the zone. Trusted conduits crossing zone boundaries must use an end-to-end secure process.

Untrusted conduits are those that are not at the same level of security as the zone endpoint. In this case the actual communication security becomes the responsibility of the individual channel.

Channels may also be trusted or untrusted. Trusted channels are communication links that allow secure communication with other security zones. A trusted channel can be used to extend a virtual security zone to include entities outside the physical security zone. Untrusted channels are communication paths that are not at the same level of security as the security zone under study. The communications to and from the reference zone (the zone that defines the communication as non-secure) must be validated before accepting the information.

[2] *ISA-62443-3-2 is currently under development. Draft copies are available to members of the ISA99 committee and other stakeholders.*

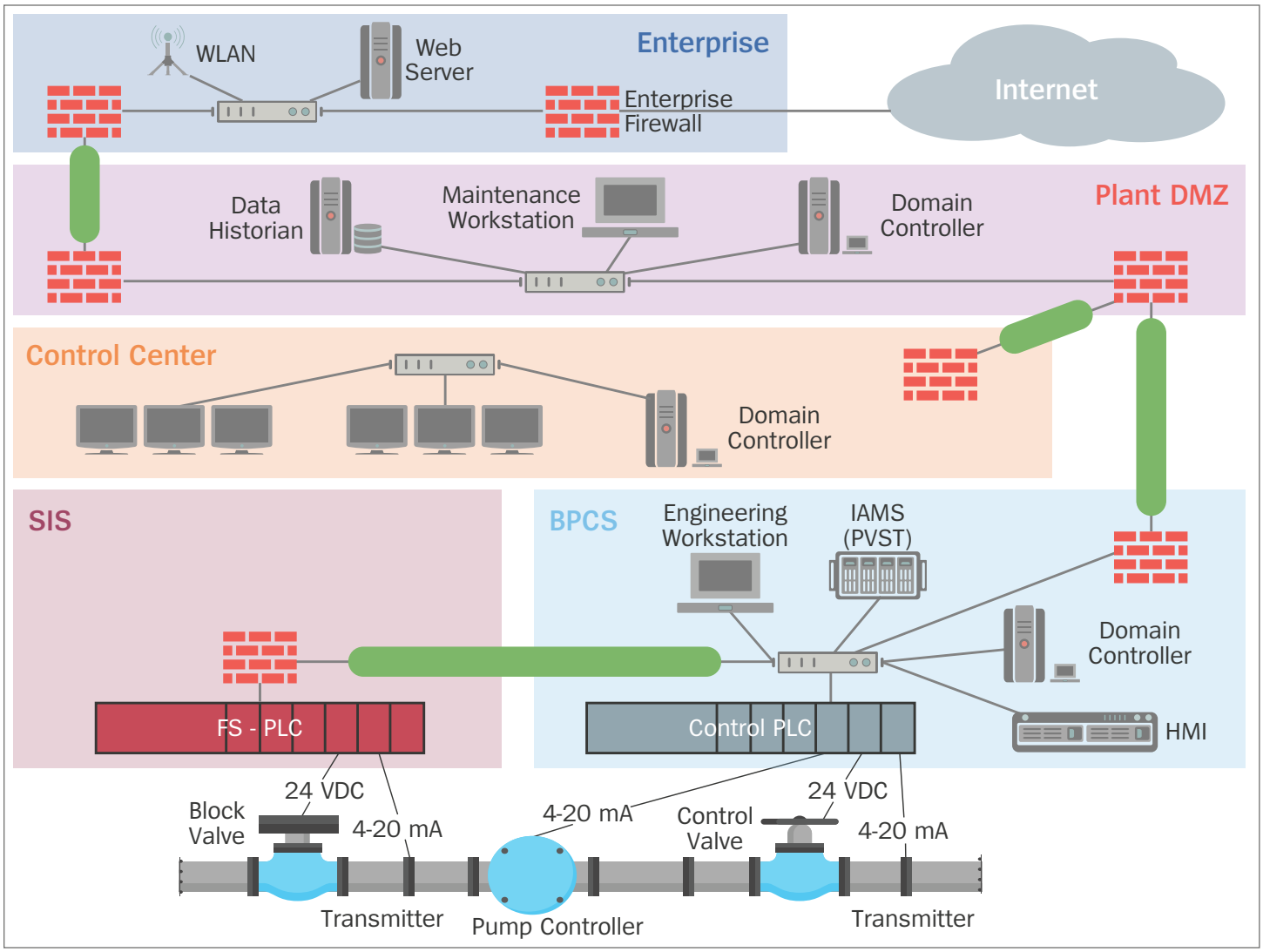

Figure 5 – Zones and Conduits Example

6.8. Describe the Zones and Conduits Model

The results of the above analysis must be captured in the form of a comprehensive model that describes each of the zones and conduits, in terms of their characteristics and behavior. Industry standards and associated case studies provide examples of such models.

Figure 5 is one such example of such a model. It is taken from the 62443 standards.

6.9. Select Segmentation Methods

There are several different methods, products and technologies available to implement the segmentation defined in the zones and conduits model. It is not necessary to use the same method in each case within a single system, although minimizing the number of different methods may reduce cost and operational complexity. Typical choices include:

- **Switches and Routers** – These devices may be sufficient in cases where the need is restricted to protected systems from uncontrolled traffic on a single network segment.
- **Firewalls** – These devices are commonly employed to separate industrial and business systems zones. Depending on the nature of the separation, they may have to provide the ability to do deep packet inspection.
- **Gateways** – Unidirectional gateways (i.e., "data diodes") are often used in cases where software-based separation is deemed insufficient to meet the requirements.
- **Virtual Networks** – Virtual local area networks (VLANs) restrict access to particular segments of the network. Policies for endpoint types, security and compliance postures and end-user access privileges can be used to determine appropriate network segments to which the endpoint can gain access.

Other methods and tools are also available, with new ones announced regularly by a variety of suppliers. They may be hardware or software based, or a combination of both.

6.9.1. Other Factors

In addition to accomplishing the necessary segmentation or separation, there are other factors that should be considered during the selection process. The need for additional capabilities depends on the requirements defined for a specific situation. Such capabilities include:

- **Implementation Cost** – Cost is also a major consideration in the selection of products and technology. In cases such as system segmentation the number of devices or software instances that may be required make it essential to consider the cost of implementation, as well as initial acquisition.

- **Operational Complexity** – Depending on the nature of the segmentation design, regular operation of the resulting systems may be more or less complex and challenging. Such complexity will add to cost of ownership over the entire life cycle. If the operational needs are overly complex, it may be tempting try to disable or bypass the protections provided.
- **Visualization** – System configurations seldom remain unchanged over time. Planned changes are often made in response to changes in system behavior. This behavior can only be monitored if the infrastructure includes the ability to visualize normal operation (i.e., network traffic, etc.).
- **Data Protection** – There are some cases where it may be necessary to protect, or obscure data exchanged between or even within zones. This is typically accomplished through some sort of data encryption.
- **Device Visibility** – Devices may also require protection, to avoid making them a target of attack. This can be accomplished by using methods to make them "invisible" on the network.

6.10. Implement and Test

Implementation and testing involves applying the specific technologies and products selected, in a manner consistent with the segmentation strategy and zone and conduit model. In all but the simplest cases, such implementation should be planned and executed using a rigorous management of change methodology.

6.11. Monitor and Adjust

Ongoing monitoring of the resulting infrastructure is essential, to identify performance or other problems that must be addressed.

7. What's Next?

Although there has been considerable progress made in the application of network segmentation and related concepts to industrial systems, there are several opportunities that still must be addressed to make lasting progress in improving their security.

7.1. Better Data Flow Models

To develop the optimum segmentation model of zones and conduits, it is essential to have a complete and thorough understanding of all data flows, both within the control system, and between it and external systems. Unfortunately, with systems that have evolved over time this understanding may not exist. In such cases it may be necessary to use some sort of monitoring or scanning tools to determine the data flows and interactions. Suppliers are now developing and supplying such tools that can be safely applied, without a risk of process upset.

7.2. Segmentation by Design

As effective approaches to segmenting complex industrial systems become more common, it is reasonable to assume that product supplier and systems integrators will develop and deliver new systems with such segmentation as a key factor in the design. This will be an important example of the "secure by design" principle. System integrators already have the ability to do this in many situations, such as the implementation of a basic control system with an associated safety system.

7.3. Improved Methods and Technology

It is reasonable to expect that the products and technologies used for system segmentation will continue to improve. Entirely new approaches may emerge based on the results of research and development.

In addition to technical capability, improvements are also required in implementation methods and techniques. For example, there is currently no formal framework that describes how to break an infrastructure into individual components, build connections between the relevant components, and apply models for complete traffic separation.

For more information please email us at Stealth@unisys.com.

8. About the Author

Eric Cosman is the Co-Chair of the ISA99 Committee on Industrial Automation and Control Systems Security which authored the ISA-62443 standard. For several years he has been heavily engaged in various areas of industrial information systems security, including:

- Former Operations IT Fellow at The Dow Chemical Company
- Founding member of the Chemical Sector Cyber Security Program of the American Chemistry Council (ACC)
- Chemical sector representative to the Industrial Control Systems Joint Working Group (ICSJWG)
- Past Vice President of Standards and Practices for the International Society of Automation (ISA)

9. References

Belden. (2014, September 24). *ICS Security for Oil and Gas Applications*. Retrieved from Belden: http://www.belden.com/blog/industrialsecurity/ICS-Security-for-Oil-and-Gas-Applications-Part-1-of-2.cfm

Brodsky, J. (2017, July 27). *Understanding Industrial Process Control.* Retrieved from SCADAS.EC: http://scadamag.infracritical.com/index.php/2017/07/27/how-a-process-works/

Byres, E. (n.d.). *Using ANSI/ISA-99 standards to improve control system security*. Retrieved from Industrial Ethernet Book: http://www.iebmedia.com/ethernet.php?id=8460&parentid=74&themeid=255&showdetail=true

Cisco. (n.d.). *A Framework to Protect Data Through Segmentation*. Retrieved from Cisco: https://www.cisco.com/c/en/us/about/security-center/framework-segmentation.html

Committee, I. (n.d.). ISA-62443-3-2: *Security for Industrial Automation and Control Systems; Part 1: Terminology, Concepts, and Models.*

Cusimano, J., & Cammack, G. (2013, August 23). *The ICS Cybersecurity Lifecycle.* Retrieved from Exida: http://www.exida.com/Resources/Whitepapers/The-ICS-Cybersecurity-Lifecycle

French, D. (2017). *Breaking Down Industrial Cybersecurity Standards.* Retrieved from Anixter: https://www.anixter.com/en_us/resources/literature/techbriefs/breaking-down-industrial-cybersecurity-standards.html

ISA99 Committee. (2007). ISA-62443-1-1: *Security for Industrial Automation and Control Systems; Terminology, Concepts, and Models.* ISA.

ISA99 Committee. (TBD). ISA-62443-3-2: *Security for industrial automation and control systems - Security Risk Assessment, System Partitioning and Security Levels.* ISA.

Knapp, E. (2014, January 6). *Implementing ICS Digital Zone Separation*. Retrieved from ISS Source: http://www.isssource.com/implementing-ics-digital-zone-separation/

Peterson, B. (2016, February 5). *Secure Network Design: Micro Segmentation.* Retrieved from SANS: https://www.sans.org/reading-room/whitepapers/bestprac/secure-network-design-micro-segmentation-36775

Tofino Security. (2012, May). *Using ANSI/ISA-99 Standards to Improve Control System Security*. Retrieved from Tofino: https://www.tofinosecurity.com/system/files/Professional/White-papers/Using-ANSI-ISA-99-Standards-WP-May-2012.pdf

Wolfgang, M., & Reichenberg, N. (2014, November 24). Segmenting for security: Five steps to protect your network. *Network World*. https://www.networkworld.com/article/2851677/security/segmenting-for-security-five-steps-to-protect-your-network.html

For more information visit www.unisys.com

Printed in the United States of America 12/17 17-0722